

Cloud Security Using ML

Literature Review Research Methods

Date: 12-12-2021

Supervisor: Massoud Zolgharni Name: Abhay Jadav

ID: 21474963

1. **Abstract**

Cloud computing has been a fast-developing field among major running businesses. The development of this field comes with many security concerns which needs to be detected and eliminated. This literature review focuses on the threats that can occur to a organization based on cloud and also focuses on the solution that can be provided for overcoming those threats. The aim of this research is for detecting as much possible threats by training data and analyzing network for detecting unusual patterns on network for detecting threats with the help of machine learning and further technologies which fits the best. The steps that I will be following in this research is by creating ML model which is trained particularly for detecting threats. I have even planned to update those unusual threats on network which could help preventing same threat to occur on any other cloud network. For conducting this research, on initial basis I have chosen few research papers which focus on the security and concerns on a cloud environment and describes the ways for overcoming them. Along with this, in this research I have planned for creating a ML model based on regression model (can be updated) for implementing my concepts.

1. **Introduction**

Cloud computing is one of the most trending technology in this era. Most of the organizations are now depending on cloud environment. Because of the surge in use of this technology has even led to many security breaches which can cause serious damage to an organization. (ALI BOU NASSIF, 2021) The threats covered are data breaches, cloud visibility DDoS attack, unauthorized access management, account hacking, Data loss and Malware Injection. (Deepak R Bharadwaj, 2018) There are many other threats which can cause severe affect on cloud network which will be included in the model of this research module. Cloud network will be secured on basis of the logs which can be extracted by various tools and by examining those logs, we will be able to build the model. (Deepak R Bharadwaj, 2018)

1. **Literature Review**

This literature review will go through all the necessary information that is required for creating a ML model. It is made up of six different research papers in which the first research papers discuss about the growing concerns in cloud security in which the threats which can be faced in future are explained. (Derrick Sampson, 2021) Further, we will be exploring the possible threats on a private cloud network as the model that we aim to develop is based on organizational data. The research done by Liu Qing and their team explains perfectly about every possible threat which we could take in consideration while developing our model. This research paper will enlighten the seriousness of threats along with the ways to be aware of these threats. (Liu Qing, 2018) The third research paper focuses of the field of creating structures to prevent these threats. It will help us in understanding the defence control hierarchy and the services that can be used for securing cloud network. It will further discuss about different services like IaaS (Infrastructure as a System), PaaS (Platform as a Service) and SaaS (Security as a Service). (Deepak R Bharadwaj, 2018) In this literature, we have also discussed about SIEM (Security Incident Event Management). The way for implementing this service in SECaaS (Security as a Service) will also be discussed further. (Jong-Hoon Lee, 2017) The concept of implementing Machine Learning as a Service in cloud network is being systematically reviewed with the help of two different research papers. The approaches used in both papers are different but somewhat similar which will help us in knowing various methodologies that can be used in providing ML as security service. The first paper focuses on few basic attacks which are totally based on network such as Adversarial attacks, Backdoor attacks, Data manipulation attacks, Evasion attacks, Exploration attacks, Model extraction attacks, Model inversion attacks, Model-reuse attacks, and Trojan attacks. It is based on 37 different articles among which majority of the research focuses on different attack whereas 6 articles aim for the defence to those attacks. (Adnan Qayyum, 2020) The second research papers that we will be using in is resulted from 63 case studies and the focus of this research paper is divided into 3 different areas which is the various types of threats in cloud network, ML techniques that will be used in securing those threats and the last segment aims on the accuracy of the model that is created. The datasets that are used in conducting these studies are from KDD and KDD CUP’99 which has proven to be most accurate in terms of results. (ALI BOU NASSIF, 2021)

1. **Concerns of Cloud Security**

There are many threats can affect a cloud network among those one of the most serious threats is data breach. Data breaches in any organization can lead to end of an organization. In the first article, the author has discussed about real life of data breaches and the effects that it has done to the organization. One of the most interesting case is about a amazon employ which has been accused for leaking data of 106 million credit cards and along with that most of their personal details has also been leaked to hackers. (Derrick Sampson, 2021)This kind of data breaches can lead into serious consequences which can even lead into failure of organizations. It is important to make sure of these loopholes and solve it as soon as possible.

1. **Threats on Cloud Network**

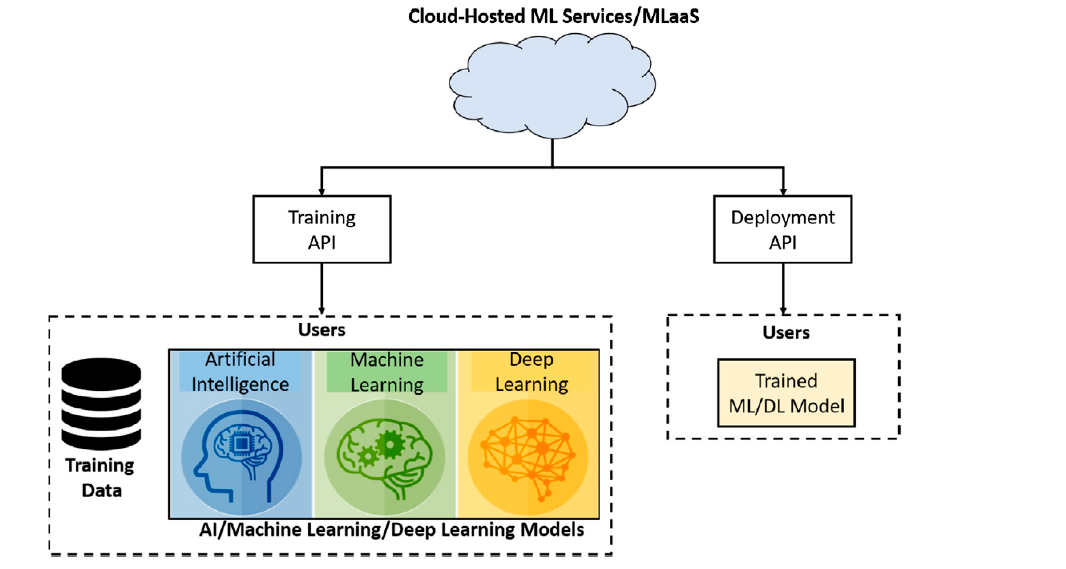
As we dive into cloud computing, the challenges are increased when compared with the traditional system. It can be classified into three segments, the first one is dynamic environment. As the nature of cloud computing is to work dynamically, it can be one of the concerns for securing as most of the data will be stored online and will travel through different network services. For overcoming these problems, it is important to test the system on regular basis which will help us in detecting loophole. (Deepak R Bharadwaj, 2018) The second concern of a cloud network is the distribution its servers. As it is distributed at many different locations, it makes it difficult in managing those data. The third concern is regarding the physical security. For a organization which is based on cloud, all of its data will be stored at a remote location which needs to be secured properly. If any intruder gets access to those servers , it can lead into data breaches. Poor access management can lead to account hijacking, data breaches, malicious insider, and insufficient due diligence (Deepak R Bharadwaj, 2018) Workload threats can be counted on basis of the amount of work that is being run on a cloud environment. If the structure of the cloud is not designed properly, it can lead to overload on servers which can result in server crashes. Many times, such crashes can also be done by introducing untrusted API on servers, so it is important to keep the network restricted. (Deepak R Bharadwaj, 2018)

1. **SECaaS (Security as a Service)**

SECaaS is a service which is used for handling footprints of a network. It works on basis of logs that are recorded and later analyzed. On basis of these analysis, the services create patterns which are classified into different segments. With the help of these services, it becomes easy for finding unusual patterns on network. The system that is being used in traditional system is SIEM (Security Information and Event Management) (Jong-Hoon Lee, 2017) This service works by collecting and analyzing data from different access logs of database such as IP stats, port status, signature stats and country stats. With the help of these logs, it will be easy for detecting unusual threats and eliminate it. We can even know the origin of attack route, regional information and the purpose of attack.

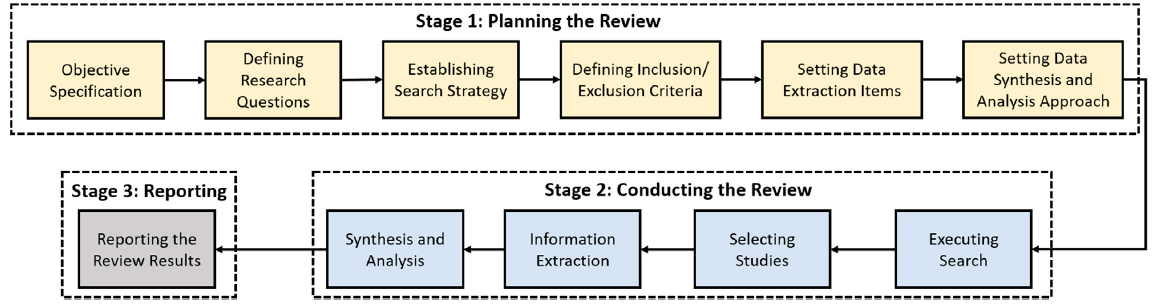
1. **Systematic Approach for Cloud ML Security**

Modern machine learning (ML) technologies are now widely used in many industries, exceeding prior best practices in a variety of fields. Face and object detection are examples of picture categorization. It takes a lot of time and resources to use these ML approaches, particularly DL-based techniques, to fulfill a given job with high performance. To train deep learning models on huge datasets, high-performance graphics processing units and tensor processing units are often used. Accordingly, since small firms and individuals cannot afford the computational resources required for Tensor Processing Units, deep model training is frequently outsourced to cloud computing services known as "Machine Learning As a Service." (Adnan Qayyum, 2020)



The process of planning and making these models will be based on datasets and two different API will be developed. The first API will be related for training dataset which will work on AI, ML and DL technologies. The approach for training data will be discussed further and once the datasets are trained, a deployment model will be build which will be placed on actual cloud network. It is necessary to keep the trained model to be updated regularly.

1. **Deployment Plans**

****

The steps for creating model will be as following in which the first stage will contain data screening. Data screening is done by understanding the objective specification. Further it will go through carious steps which are mainly focused on preparing data in a usable format which can be further used as input for deployment of the model. (Adnan Qayyum, 2020) The ML models which will be used for deployment are SVM, Random Forest, KNN, Decision tree and Linear Regression. Among all these models, the most accurate model is said to be SVM. (ALI BOU NASSIF, 2021) It is also one of the most frequent used model trained for securing cloud is efficient. Further, for enhancing the security we can implement hybrid models which can be created by adding two different ML models. (ALI BOU NASSIF, 2021)

1. **Conclusion**

This literature review explains about the basics of ML for creating ML model for securing cloud network. It goes through threats among cloud computing, later it expands into specific threats which a private cloud organization can face and the consequences that can occurs due to it. It also discusses about the services which can be helpful in providing security in cloud. For implementing ML model, a systematic approach is also explained in this review. It is mainly based on six different research papers which are specifically for securing cloud network and these research is conducted on basis of more than 100 articles.

# Bibliography

Adnan Qayyum, A. I. M. U. W. I. J. Q., 2020. *Securing Machine Learning in the,* USA: IEEE Xplore.

ALI BOU NASSIF, M. A. T. Q. N. H. A., 2021. *Machine Learning for Cloud Security: A Systematic Review,* Shahraj: IEEE Access.

Deepak R Bharadwaj, A. B. M. C., 2018. *Cloud Threat Defense – a Threat Protection and,* Banglore: IEEE Xplore.

Derrick Sampson, M. M. C., 2021. *The Growing Security Concerns of Cloud Computing,* East Stroudsburg, PA, USA: IEEE Xplore.

Jong-Hoon Lee, Y. S. K. J. H. K. I. K. K., 2017. *Toward the SIEM Architecture,* Daejeon, Korea: IEEE.

Liu Qing, Z. B. W. J. L. Q., 2018. *Research on Key Technology of Network Security Situation Awareness of Private,* Beijing, China: IEEE International Conference.